Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
06/06/2019	1.0	M. Elbanhawi	First submissio

Table of Contents

Purpose of the Technical Safety Concept

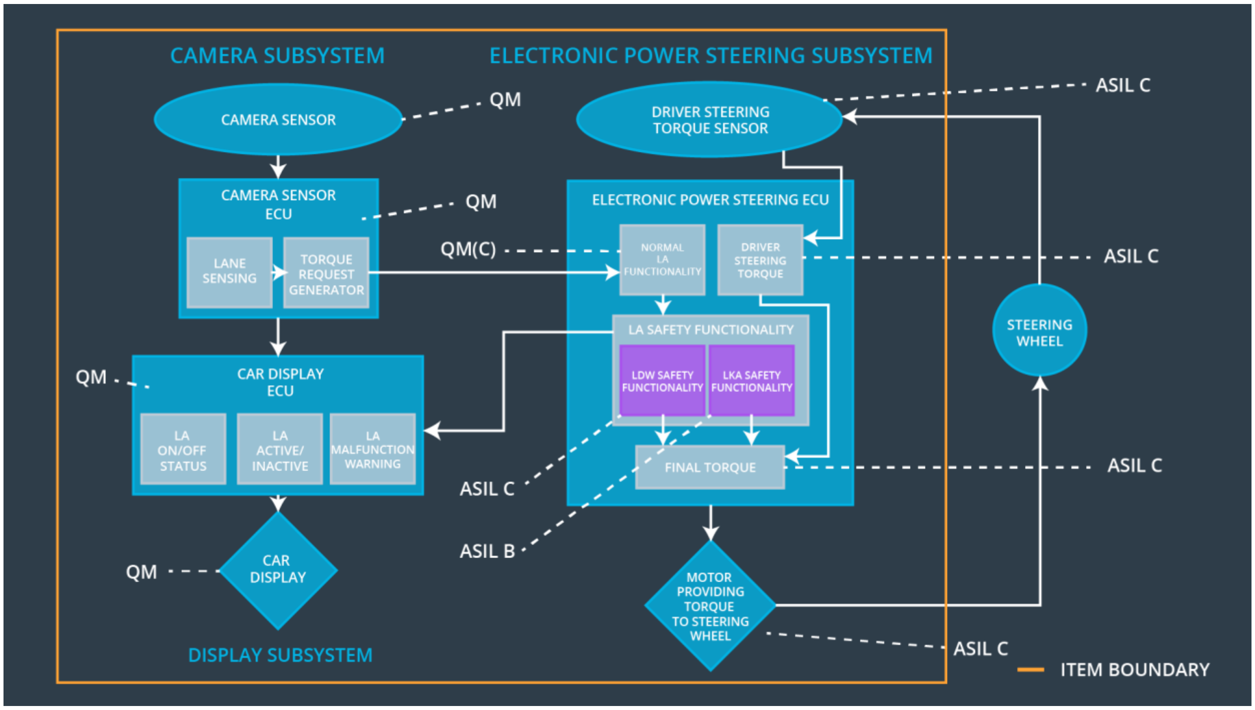
[Instructions: Answer what is the purpose of a technical safety concept?]

Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Disable system
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Disable system
Functional Safety Requirement 02-01	The electronic power steering ECU shall limit lane keeping assistance torque for only Max_Duration	B	500 ms	Disable system.

Refined System Architecture from Functional Safety Concept

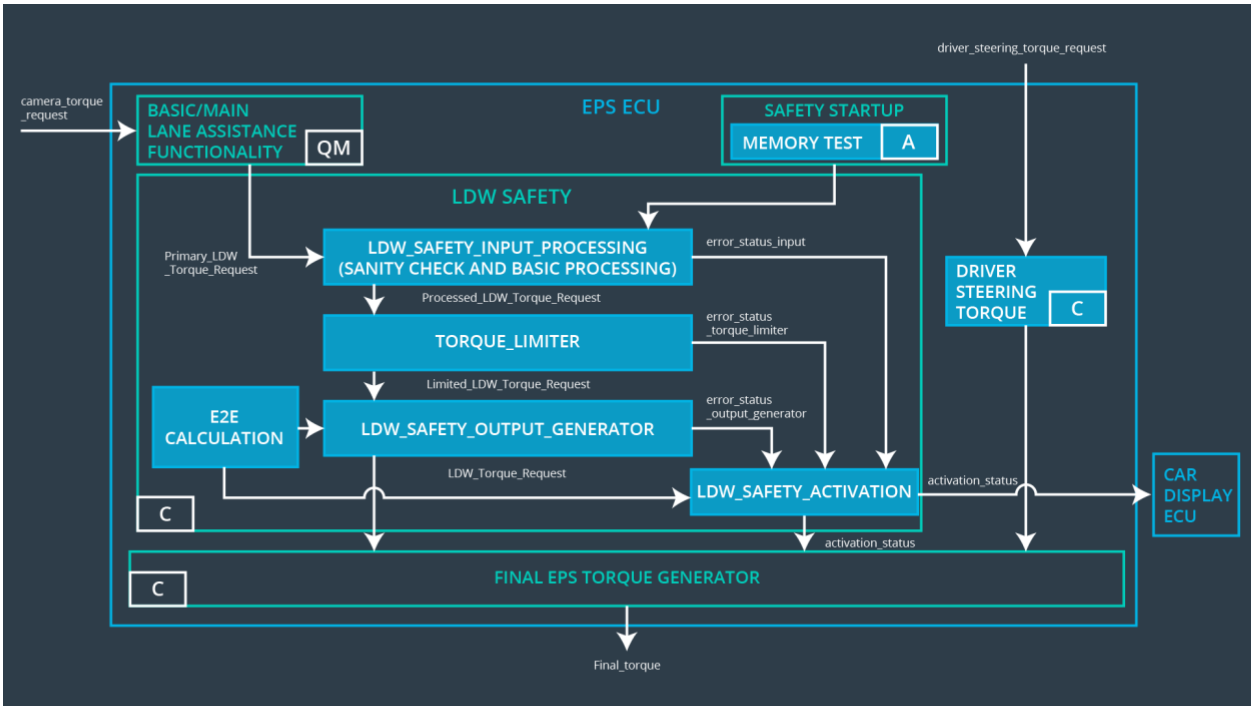


Functional overview of architecture elements

Element	Description
Camera Sensor	Capture images of the road and send to the camera ECU
Camera Sensor ECU - Lane Sensing	Software module that processes images to determine lane and position of vehicle in lane
Camera Sensor ECU - Torque request generator	Software module the sends a torque request based on the lane sensing output to the power steering ECU
Car Display	HMI to the driver, displays light status for LKA and LDW
Car Display ECU - Lane Assistance On/Off Status	Indicates the status of Lane Assistance
Car Display ECU - Lane Assistant Active/Inactive	Indicates the activity of Lane Assistance

Car Display ECU - Lane Assistance malfunction warning	Indicates the functionality of Lane Assistance
Driver Steering Torque Sensor	Measures the steering input from the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software block that receives torque input from the driver
EPS ECU - Normal Lane Assistance Functionality	Software block that receives torque request from Camera Sensor ECU – Torque request block
EPS ECU - Lane Departure Warning Safety Functionality	Software block that constrains the torque amplitude and frequency to Max_Torque_Amplitude and Max_Torque_Frequency respectively.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software block that limits the LKA activity duration to Max_Duration
EPS ECU - Final Torque	Software block that combines torque request from LKA, LDW and send it to the motor
Motor	Applies torque request to the steering wheel

Technical Safety Concept



driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements
(derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	X		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The Torque Limiter component shall limit the Limited_LDW_Torque_Request amplitude is below Max_Torque_Amplitude	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 02	The LDW_Safety_Output_Generator component shall limit the LDW_Torque_Request amplitude is below Max_Torque_Amplitude	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 03	The Torque Limiter component shall output an error if the Limited_LDW_Torque_Request amplitude is above Max_Torque_Amplitude	C	50ms	LDW Safety	Deactivate LDW
Technical Safety	The LDW_Safety_Output_Generato	C	50ms	LDW Safety	Deactivate LDW

Requirement 04	r component shall output an error if LDW_Frequency_Request amplitude is above Max_Torque_Amplitude				
Technical Safety Requirement 05	The LDW_SAFETY_ACTIVATION component shall deactivate the EPS_Torque_generator when it receives an error	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 06	The LDW_SAFETY_ACTIVATION component shall output a malfunction to the car display when it receives an error	C	50ms	LDW Safety	Deactivate LDW

Functional Safety Requirement 01-2 with its associated system elements
(derived in the functional safety concept)

ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	**Technical Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Architecture Allocation**	**Safe State**
Technical Safety	The Frequency Limiter component shall limit the	C	50ms	LDW Safety	Deactivate

Requirement 01	Limited_LDW_Frequency_Request is below Max_Torque_Frequency				LDW
Technical Safety Requirement 02	The LDW_Safety_Output_Generator component shall limit the LDW_Frequency_Request frequencyis below Max_Torque_Frequency	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 03	The Torque Limiter component shall output an error if the Limited_LDW_Frequency_Request frequency is above Max_Torque_Frequency	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 04	The LDW_Safety_Output_Generator component shall output an error if LDW_Frequency_Request frequency is above Max_Torque_Frequency	A	Ignition	LDW Safety	Deactivate LDW
Technical Safety Requirement 05	The LDW_SAFETY_ACTIVATION component shall deactivate the EPS_Torque_generator when it receives an error	C	50ms	LDW Safety	Deactivate LDW
Technical Safety Requirement 06	The LDW_SAFETY_ACTIVATION component shall output a malfunction to the car display when it receives an error	C	50ms	LDW Safety	Deactivate LDW

Lane Keeping Assistance (LKA) Requirements:

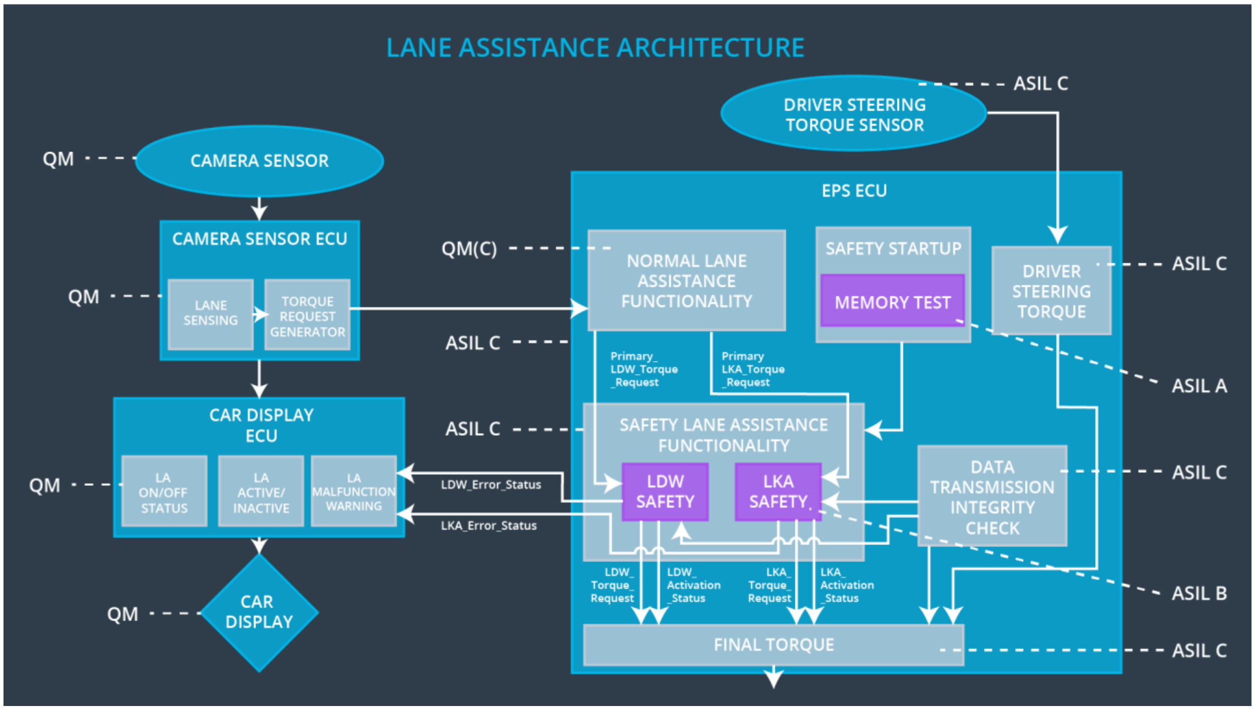
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LKA_Torque_Request duration shall be below Max_Duration.	B	500ms	LKA Safety	Deactivate LKA
Technical Safety Requirement 02	The LKA Safety component shall output an error if the duration LKA_Torque_Request is above Max_Duration.	B	500ms	LKA Safety	Deactivate LKA
Technical Safety Requirement 03	A Safety test shall be conducted on the memory on start up	B	Igniton	LKA Safety	Deactivate LKA
Technical Safety Requirement 04	The LKA_Safety component shall deactivate the EPS_Torque_generator when it receives an error	B	500ms	LKA Safety	Deactivate LKA
Technical Safety Requirement 05	The LKA_Safety component shall output a malfunction to the car display when it receives an error	B	500ms	LKA Safety	Deactivate LKA

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The Torque Limiter component shall limit the Limited_LDW_Torque_Request amplitude is below Max_Torque_Amplitude	X		
Technical Safety Requirement 01-01-02	The LDW_Safety_Output_Generator component shall limit the LDW_Torque_Request amplitude is below Max_Torque_Amplitude	X		
Technical	The Torque Limiter component	X		

Safety Requirement 01-01-03	shall output an error if the Limited_LDW_Torque_Request amplitude is above Max_Torque_Amplitude			
Technical Safety Requirement 01-01-04	The LDW_Safety_Output_Generator component shall output an error if LDW_Frequency_Request amplitude is above Max_Torque_Amplitude	**X**		
Technical Safety Requirement 01-01-05	The LDW_SAFETY_ACTIVATION component shall deactivate the EPS_Torque_generator when it receives an error	**X**		
Technical Safety Requirement 01-01-06	The LDW_SAFETY_ACTIVATION component shall output a malfunction to the car display when it receives an error	**X**		
Technical Safety Requirement 01-02-01	The Frequency Limiter component shall limit the Limited_LDW_Frequency_Request is below Max_Torque_Frequency	**X**		
Technical Safety Requirement 01-02-02	The LDW_Safety_Output_Generator component shall limit the LDW_Frequency_Request frequencyis below Max_Torque_Frequency	**X**		
Technical Safety Requirement 01-02-03	The Torque Limiter component shall output an error if the Limited_LDW_Frequency_Request frequency is above Max_Torque_Frequency	**X**		
Technical Safety	The LDW_Safety_Output_Generator	**X**		

Requirement 01-02-04	component shall output an error if LDW_Frequency_Request frequency is above Max_Torque_Frequency			
Technical Safety Requirement 01-02-05	The LDW_SAFETY_ACTIVATION component shall deactivate the EPS_Torque_generator when it receives an error	**X**		
Technical Safety Requirement 02-01-01	The LKA_Torque_Request duration shall be below Max_Duration.	**X**		
Technical Safety Requirement 02-01-02	The LKA Safety component shall output an error if the duration LKA_Torque_Request is above Max_Duration.	**X**		
Technical Safety Requirement 02-01-03	A Safety test shall be conducted on the memory on start up	**X**		
Technical Safety Requirement 02-01-04	The LKA_Safety component shall deactivate the EPS_Torque_generator when it receives an error	**X**		
Technical Safety Requirement 02-01-05	The LKA_Safety component shall output a malfunction to the car display when it receives an error	**X**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Disable LDW	Malfunction_01, Malfunction_02,	Yes	LDW Malfunction Warning on Car

				Display
WDC-02	Disable LKW	Malfunction_03,	Yes	LKA Malfunction Warning on Car Display